ГОЛОВІ СПЕЦІАЛІЗОВАНОЇ ВЧЕНОЇ РАДИ Д 26.062.17

НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ

03680, Київ, пр. Космонавта Комарова, 1.

ВІДГУК

офіційного опонента
завідувач кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету доктора технічних наук, професора Рудницького Володимира Миколайовича
на дисертаційну Навроцького Дениса Олександровича «Методи побудови симетричних криптографічних шифрів з використанням тривимірних перетворень», подану на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – Системи захисту інформації

Актуальність теми дисертації. Розвиток інформаційних технологій і широке використання компьютерних та інформаційно-телекомунікаційних систем практично у всіх сферах життєдіяльності суспільства, провів до стрімкого зростання обсягів даних, що обробляються і передаються, розробки та неконтрольованого розповсюдження програмного забезпечення.

На сьогоднішній день актуальними стають задачі підвищення якості та ефективності систем інформаційної безпеки. Одним із перспективних напрямів рішення даних задач є розвиток криптографічних методів та засобів захисту інформації.

В галузі інформаційної безпеки актуальними є питання забезпечення швидкості криптографічних перетворень великих обсягів даних, високого рівня стійкості сучасних методів криптоаналізу, комплексного підвищення безпеки й достовірності отримання інформації. Однак деякі існуючі в державі комплекси криптографічного захисту на сьогоднішній день морально й фізично застаріли й не забезпечують виконання сучасних ймовірносно-часових вимог. Крім того актуальним залишається цілий ряд задач, зокрема, розробка крипто примітивів орієнтованих на короткострокові та довгострокові перспективи розвитку обчислювальної техніки, побудова крипто примітивів для обробки великої кількості даних, розробка методів використання крипто примітивів в алгоритмах

та інші. Вирішення поставлених задач забезпечить підвищення якості та ефективності систем інформаційної безпеки.

Дисертаційна робота виконувалась відповідно до основних наукових напрямів і найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2014 – 2018 рр., а саме: п.1.2.8.1 «Розробка методів та інформаційних технологій розв'язання задач комп'ютерної криптографії та стеганографії»; Стратегії національної безпеки України від 26 травня 2015 року № 287/2015 а саме: п.4.12 «Забезпечення кібербезпеки і безпеки інформаційних ресурсів, зокрема реформування системи технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС з досліджень та інновацій;), а також держбюджетної НДР «Розробка та впровадження програмних засобів захисту інформації від несанкціонованого доступу в електронних системах документообігу у вищих навчальних закладах України» (номер державної реєстрації 0110U000222)), в якій дисертант був виконавцем.

Тому вважаю, що тема дисертаційного дослідження «Методи побудови симетричних криптографічних шифрів з використанням тривимірних перетворень» та вирішена у роботі наукова задача підвищення якості криптографічного захисту інформації на основі застосування нових блокових і потокових шифрів з використанням динамічно керованих тривимірних криптографічних примітивів є *актуальними*.

2. Наукова новизна результатів роботи

У роботі досліджено підвищення якості функціонування систем криптографічного захисту інформаційних ресурсів за рахунок розробки та застосування нових блокових і потокових шифрів з використанням динамічно керованих тривимірних криптографічних примітивів

До основних нових наукових результатів, отриманих в дисертації, на мою думку, слід віднести наступні.

– уперше розроблено метод формування сукупності динамічно керованих примітивів на основі узагальнених перетворень Грея та матриць Галуа для тривимірного простору, які за рахунок розроблених динамічних дискретних математичних моделей перетворень в тривимірному просторі забезпечили збільшенні швидкості і стійкості шифрів при обмеженні на об'єм пам'яті;

– удосконалено метод синтезу матриць для таблиць підстановки і перестановки на основі запропонованих тривимірних криптографічних примітивів,

що забезпечило розширення множини узагальнених генераторів псевдовипадкових послідовностей, та побудову нових алгоритмів формування таємних ключів шифрування для мереж з відкритими каналами зв'язку;

– отримали подальший розвиток методи розробки засобів захисту командно-телеметричної та відеоінформації в каналах зв'язку за рахунок методів симетричного блокового тривимірного криптографічного перетворення інформації з динамічно керованими параметрами шифрування, що дало можливість модифікації параметрів криптографічних примітивів при переході до чергового блоку інформації, що шифрується.

Практичне значення отриманих результатів. Практична цінність роботи полягає в доведенні здобувачем отриманих наукових результатів до конкретних інженерних методик, алгоритмів, моделей та варіантів функціонування криптографічних систем захисту інформації.

На підставі проведених досліджень одержано такі практичні результати: побудовано алгоритми функціонування, структури та математичні моделі реалізації криптосистем і крипто примітивів тривимірного простору, отримано 9 патентів України на «Спосіб криптографічного захисту інформації», що в сукупності дає можливість підвищувати якість систем захисту інформації.

Практична цінність роботи підтверджена актами впровадження основних результатів дослідження.

Реалізація. Дисертаційна робота виконувалася відповідно до плану НДР Національного авіаційного університету. Одержані в ній теоретичні й практичні результати впроваджено

- у навчальному процесі кафедри електроніки Національного авіаційного університету, кафедри виробництва приладів Національного технічного університету України «КПІ» імені Ігоря Сікорського»,
- у науково-технічних розробках ТОВ «Агфар», ТОВ «Гратис, Лтд».

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації.

У вступі до дисертаційної роботи наведена актуальність теми, поставлені наукові задачі, які необхідно вирішити для досягнення мети роботи, визначена практична значимість отриманих результатів.

У першому розділі проведено аналіз криптографічних методів захисту інформації за стійкостю, швидкістю та вимогами до ресурсів, обґрунтовані шляхи

вдосконалення алгоритмів симетричного шифрування. Виявлені переваги і недоліки діючих вітчизняних та зарубіжних стандартів блокового шифрування. Проведено аналіз найбільше поширених типів атак, яким повинні протидіяти крипто примітиви та крипто алгоритми що розробляються в дисертаційному дослідження.

Другий розділ дисертації присвячений розробці моделей та методів динамічного перетворення інформації в тривимірному просторі. Будуються тривимірні моделі лінійного розсіювання, нелінійної заміни та «ковзного кодуванню» на основі узагальнених перетворень Грея та матриць Галуа. Будуються моделі перестановок в тривимірному просторі

Третій розділ присвячений розробці криптографічних примітивів для реалізації в тривимірному просторі. Отримані математичні моделі та методи динамічного перетворення інформації уточнюються та деталізуються з урахуванням особливостей реалізації блокового та потокового шифрування. Розробляється структура крипто алгоритму на основі побудованих тривимірних крипто примітивів.

У четвертому розділі проводиться теоретична та практична оцінка реалізації розроблених в дисертаційному дослідження методів побудови тривимірних симетричних криптографічних шифрів. Наводяться результати перевірки та лабораторних досліджень розробленого апаратно-програмного забезпечення, яке реалізує отримані наукові результати.

У додатках наведено текст програмної реалізації шифру, результати статистичного дослідження згенерованих шифром послідовностей, акти впровадження.

Апробація результатів дисертаційних досліджень. Результати дисертаційної роботи доповідалися й обговорювалися на міжнародній науково-технічній конференції «Захист інформації і безпека інформаційних систем» (Львів, 2012); всеукраїнській науково-практичній конференції «Проблеми та перспективи розвитку авіації та космонавтики» (Київ, 2012); науково-технічній конференції «Наукоємні технології» (Київ, 2012); міжнародній науково-технічній конференції «АВІА–2013» (Київ, 2013); всеукраїнській науково-практичній конференції «Проблеми навігації і управління рухом» (Київ, 2013); міжнародній науково-технічній конференції «Розвиток наукових досліджень 2013» (Полтава, 2013); науково-технічній конференції «Проблеми розвитку глобальної системи зв’язку, навігації, спостереження та організації повітряного руху CNS/ATM» (Київ, 2014);

міжнародній науково-технічній конференції «ITSEC» (Київ, 2015); міжнародній науково-технічнаій конференція «ABIA–2015» (Київ, 2015); науково-практична конференція «Сучасні тенденції розвитку системного програмування» (Київ, 2015).

Методи досліджень. Проведені дослідження ґрунтуються на теорії криптографічного захисту інформації, теорії чисел, алгебричній теорії груп, полях Галуа, теорії незвідних і примітивних поліномів, також теорії синтезу генераторів псевдовипадкових послідовностей, теорії ймовірностей та математичній статистиці, об'єктно-орієнтованого програмування.

Вибір методів дослідження забезпечив **достовірність отриманих результатів** та висновків, що підтверджується збіжністю результатів експериментальних досліджень, отриманих під час імітаційного моделювання з теоретичними і практичними результатами. Все це знайшло своє відображення у публікаціях та обумовлено їх відповідністю положенням теорії кодування та захисту інформації.

Завершеність роботи, стиль викладання матеріалу, публікації та апробація результатів досліджень. Аналіз сукупності наукових результатів, представлених в роботі Навроцького Дениса Олександровича, засвідчує особистий внесок автора в науку щодо удосконалення відповідних математичних моделей, методів та засобів криптографічного перетворення в тривимірному просторі.

Дисертаційна робота написана грамотно, науково-технічна термінологія в цілому використовується коректно. Стиль викладу матеріалів дисертації зрозумілий і досить логічний.

Основні результати дисертаційних досліджень з достатньою повнотою опубліковані в 32 друкованих працях, у тому числі 12 статтях у наукових журналах і збірниках наукових праць, внесених до списку фахових видань України, 1 статті яка входить у наукометричну базу Scopus, а також 10 тезах доповідей на наукових конференціях та 9 патентах України на корисну модель.

Дисертаційна робота повністю відповідає положенням паспорту спеціальності 05.13.21 – Системи захисту інформації.

Зміст автореферату ідентичний основним положенням та висновкам дисертації.

Зауваження по дисертації:

1. Вибір автором тривимірної архітектури побудови криптоалгоритмів та крипто

примітивів на мою думку оправданий лише з практичної точки зору і то при апаратній реалізації. Розроблені автором моделі і методи, по своїй сутності забезпечують побудову криптоалгоритмів та крипто примітивів в *n*-мірному просторі, а збільшення кількості степенів свободи даних забезпечить підвищення ефективності їх шифрування.

2. У вступі до дисертації, а також автореферату при формулюванні задач, наукової новизни та практичного значення отриманих результатів вводяться позначення умовних скорочень, не зважаючи на те що в роботі присутній «Перелік умовних скорочень, символів, скорочень і термінів». Надмірна деталізація мети та наукової новизни ускладнює сприйняття їх сутності.
3. Дисертаційна робота має деякі недоліки по структурі, а також невагомі неточності. Наприклад: и розділ 1 дисертації (32 ст.) перевантажений описом відомих методів криптографічного захисту інформації, стандартів блокового шифрування, описом атак на крипто алгоритми Даний розділ доцільно було б скоротити на 25-40% за рахунок зменшення рівня деталізації відомих прикладів та більшої структуризації матеріалу; не зрозуміло, навіщо автор в підрозділах 2.1 розглядає трансверсалі і діагоналі тривимірних матриць, якщо в подальшому дослідженні вони не використовуються; в 3 розділі викликає сумнів твердження автора, що тривимірне ковзне шифрування порівняно з одновимірним не потребує додаткових затрат машинного часу та збільшення складності алгоритму, адже при виборі наступного елемента який буде участувати в перетворенні необхідно не тільки інкрементувати один з його індексів, а знайти його фізичне розташування шляхом додавання всіх змішень, які залежать від індексів; недостатньо описана узагальнена структурна схема RSB-шифру, а її робота лише продемонстрована прикладами; в 4 розділі лише констатується що було розроблене програмне забезпечення, текст програм якого наведено в додатках. Відсутність опису особливостей програмної реалізації, та алгоритмів на основі яких розроблявся програмний продукт, значно знижує практичну цінність дисертаційного дослідження; в роботі та авторефераті присутні орфографічні та стилістичні помилки та неточності.

Вищезазначені недоліки та зауваження не впливають на загальний позитивний висновок щодо дисертації.

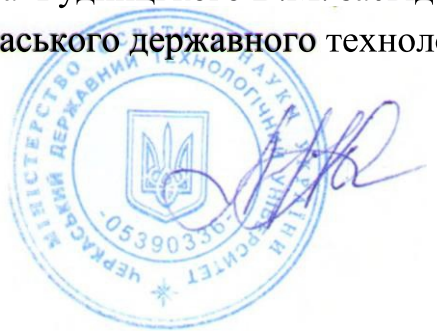
Загальні висновки. Дисертація є завершеною науково-дослідною роботою. Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю

висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота задовольняє вимогам "Порядку присудження наукових ступенів", а її автор Навроцький Денис Олександрович заслуговує присудження наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – системи захисту інформації

Офіційний опонент
завідувач кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаського державного технологічного університету,
д.т.н., професор

В. М. Рудницький

Підпис офіційного опонента Рудницького В.М. засвідчую.
Секретар Вченої ради Черкаського державного технологічного університету,
к.е.н., доцент



Лега Н.Ю.